

Notice of Allowability

Application No.

09/972,385

Examiner

Ali S. Abyaneh

Applicant(s)

RIEDEL ET AL.

Art Unit

2137

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address--

All claims being allowable, PROSECUTION ON THE MERITS IS (OR REMAINS) CLOSED in this application. If not included herewith (or previously mailed), a Notice of Allowance (PTOL-85) or other appropriate communication will be mailed in due course. **THIS NOTICE OF ALLOWABILITY IS NOT A GRANT OF PATENT RIGHTS.** This application is subject to withdrawal from issue at the initiative of the Office or upon petition by the applicant. See 37 CFR 1.313 and MPEP 1308.

1. ☒ This communication is responsive to 8/30/2007.
2. ☒ The allowed claim(s) is/are 1,3-16,18-27,30-33 and 35-39.
3. ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
- a) ☐ All b) ☐ Some* c) ☐ None of the:
1. ☐ Certified copies of the priority documents have been received.
2. ☐ Certified copies of the priority documents have been received in Application No. _____.
3. ☐ Copies of the certified copies of the priority documents have been received in this national stage application from the International Bureau (PCT Rule 17.2(a)).

* Certified copies not received: _____.

Applicant has THREE MONTHS FROM THE "MAILING DATE" of this communication to file a reply complying with the requirements noted below. Failure to timely comply will result in ABANDONMENT of this application.

THIS THREE-MONTH PERIOD IS NOT EXTENDABLE.

4. ☐ A SUBSTITUTE OATH OR DECLARATION must be submitted. Note the attached EXAMINER'S AMENDMENT or NOTICE OF INFORMAL PATENT APPLICATION (PTO-152) which gives reason(s) why the oath or declaration is deficient.
5. ☐ CORRECTED DRAWINGS (as "replacement sheets") must be submitted.
- (a) ☐ including changes required by the Notice of Draftsperson's Patent Drawing Review (PTO-948) attached
- 1) ☐ hereto or 2) ☐ to Paper No./Mail Date _____.
- (b) ☐ including changes required by the attached Examiner's Amendment / Comment or in the Office action of Paper No./Mail Date _____.
- Identifying indicia such as the application number (see 37 CFR 1.84(c)) should be written on the drawings in the front (not the back) of each sheet. Replacement sheet(s) should be labeled as such in the header according to 37 CFR 1.121(d).
6. ☐ DEPOSIT OF and/or INFORMATION about the deposit of BIOLOGICAL MATERIAL must be submitted. Note the attached Examiner's comment regarding REQUIREMENT FOR THE DEPOSIT OF BIOLOGICAL MATERIAL.

Attachment(s)

1. ☐ Notice of References Cited (PTO-892)
2. ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3. ☐ Information Disclosure Statements (PTO/SB/08), Paper No./Mail Date _____
4. ☐ Examiner's Comment Regarding Requirement for Deposit of Biological Material
5. ☐ Notice of Informal Patent Application
6. ☒ Interview Summary (PTO-413), Paper No./Mail Date _____
7. ☒ Examiner's Amendment/Comment
8. ☒ Examiner's Statement of Reasons for Allowance
9. ☐ Other _____

EXAMINER'S AMENDMENT

1. The application has been amended as follows:

An examiner's amendment to the record appears below. Should the changes and/or additions be unacceptable to applicant, an amendment may be filed as provided by 37 CFR 1.312. To ensure consideration of such an amendment, it **MUST** be submitted no later than the payment of the issue fee.

Authorization for this examiner's amendment was given in a telephone interview with applicant's attorney Philip S. Lyren on 09-17-2007.

Claim 1 has been amended to:

A method of file access control comprising:
storing an encrypted filename of a file at a location in a computing system;
converting the encrypted filename into a plaintext filename;
modifying the plaintext filename into a modified filename; and
authorizing an entity to access the file for performing a write operation on the file by comparing the modified filename to the stored encrypted filename;
wherein said converting comprises using a key that comprises a combination of two encryption keys to convert the encrypted filename into the plaintext filename.

Claim 15 has been amended to:

An apparatus for controlling access to a file, comprising:
a server for the storing an encrypted filename associated with a file; and a client in communication with the server for retrieving the encrypted filename from

the server, for converting the encrypted filename into a plaintext filename and for modifying the plaintext filename into a modified filename, wherein the client provides the modified filename to the server and wherein the server determines whether the client is authorized to perform a write operation on the file by comparing the modified filename received from the client to the stored encrypted filename; wherein said client converts the encrypted filename into the plaintext filename using a key that comprises a combination of two encryption keys.

Claim 3 has been amended to:

The method according to claim 2 1, wherein said modifying comprises using a first one of the two encryption keys to encrypt the plaintext filename into the modified filename.

Claim 5 has been amended to:

The method according to claim 2 1, wherein said modifying comprises using a first one of the two encryption keys to encrypt the plaintext filename and performing a hash function on the filename thereby forming the modified filename.

Claim 18 has been amended to:

The apparatus according to claim 47 15, wherein said client forms the modified filename using a first one of the two encryption keys to encrypt the plaintext filename.

Claim 20 has been amended to:

The apparatus according to claim ~~47~~ 15, wherein said client forms the modified filename using a first one of the two encryption keys to encrypt the plaintext filename and performs a hash function on the filename thereby forming the modified filename.

Claim 21 has been amended to:

The apparatus according to claim ~~47~~ 15, wherein said server performs a hash function on the filename to form a result and determines whether the client is authorized to perform the read operation on the file by comparing the result to a stored hash value.

Claim 22 has been amended to:

The apparatus according to claim ~~47~~ 15, wherein said client forms the modified filename using a first one of the two encryption keys to encrypt the plaintext filename and performs a hash function on the filename to form a result and wherein the server determines whether the client is authorized to perform the type of operation on the file by comparing the result to a stored hash value.

Claim 36 has been amended to:

The method according to claim 2 1, further comprising:
encrypting the plaintext filename using a key that comprises a

Art Unit: 2137

combination two encryption keys; and comparing a result of this encrypting to the stored encrypted filename to determine whether to permit read access to the file.

Claims 2 and 17 are cancelled.

Allowable Subject Matter

2. Claims 1,3-16, 18-27, 30-33 and 35-39 are allowed.

Examiner's statement for reason for allowance

The following is an examiner's statement for allowance:

The prior art Bolosky et al (U.S. Publication NO 2002/0194484) of record discloses, in a serverless distributed file system, the writer of a file can provide file authentication information to a verifying machine without having to compute a new digital signature every time a written file is closed. Periodically, the writer compiles a list of the hash values of all files that have been written over a recent interval, computes a hash of the list, and signs the hash. This signed list of hash values is known as a manifest, akin to a shipping manifest that enumerates the items in a shipment.

The prior art Hubbard et al (U.S. Patent NO 6,847,995) of record discloses, a method of operating a server system within a distributed processing system to secure transmissions within the distributed processing system, including, coupling a server system to a network that is configured to be coupled to a plurality of distributed devices, generating a security measure for electronic information to be sent from the server

system to at least one of the distributed devices, partitioning the security measure into multiple distributable portions, sending each of the multiple distributable portions to different distributed devices, and providing information to the at least one distributed device to allow the partitioned security measure to be reconstructed.

The prior art Scheidt et al (U.S. Publication NO 2002/0062451) of record discloses, a process of checking the authorization and authenticity of an application includes authenticating an application authentication file against a domain administrator's public membership key. An application executable is then hashed, and compared to an authentication hash contained in the application authentication file. Services are denied to the application if the application hash and the authentication hash do not match. If the application hash and the authentication hash match configuration assignments in the application authentication file are decoded and compared to the user's configuration assignments. Services are provided or denied to the application based on a favorable or not favorable of decoded result.

The prior art of record teaches the claimed invention substantially, but it fails to teach or suggest following limitation:

As per claim 1, authorizing an entity to access the file for performing a write operation on the file by comparing the modified filename to the stored encrypted filename; wherein said converting comprises using a key that comprises a combination of two encryption keys to convert the encrypted filename into the plaintext filename.

As per claim 15, the server determining whether the client is authorized to perform a write operation on the file by comparing the modified filename received from the client to the stored encrypted filename; wherein said client converts the encrypted filename into the plaintext filename using a key that comprises a combination of two encryption keys.

As per claim 30, wherein the server determines that the writer is authorized to write to the file by receiving from the writer the filename encrypted using the first key, encrypting the received filename again using the second key thereby forming a twice encrypted filename and comparing the twice encrypted filename to the stored encrypted filename.

As per claim 31, wherein the server determines that the writer is authorized to write to the file by receiving from the writer the filename encrypted using the first key, applying a hash function to the received filename thereby forming a computed hash value and comparing the computed hash value to a stored hash value.

As per claim 32, writer having a first key that permits the writer to write to the file and the server determining whether the writer is authorized to write to the file by receiving from the writer the filename encrypted using the second key and comparing the received filename to the second stored encrypted filename. Consequently, claim 32 is allowed over the prior art.

Any comments considered necessary by applicant must be submitted no later than the payment of the issue fee and, to avoid processing delays, should preferably


Art Unit: 2137

accompany the issue fee. Such submissions should be clearly labeled "Comments on Statement of Reasons for Allowance."

Conclusion

3. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Ali Abyaneh whose telephone number is (571) 272-7961. The examiner can normally be reached on Monday-Friday from (8:00-5:00). If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Emmanuel Moise can be reached on (571) 272-3865. The fax phone numbers for the organization where this application or proceeding is assigned as (571) 273-8300. Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Ali Abyaneh *AA*
Patent Examiner
Art Unit 2137
09/17/07


EMMANUEL L. MOISE
SUPERVISORY PATENT EXAMINER